Proposal for IEEE 802.1CQ (Self-Assignment part)	
Author	**Affiliation**
Antonio de la Oliva	University Carlos III of Madrid, InterDigital
Robert Gazda	InterDigital
Any Other	
Abstract: This contribution proposes text and new message formats for the Self-Assignment of MAC addresses in IEEE 802.1CQ	

Introduction

This document addresses the scope of IEEE 802.1CQ which aims at providing a way at layer 2 to automatically assign local MAC addresses in the SAI space as defined by the recently published IEEE 802c [REF].

The IEEE 802.1CQ purpose is to address the automatic assignment of MAC addresses in an IEEE 802 network. In order to do so, several options exist. Basically, two ways of MAC address assignment have been explored, self assignment (**the so-called Claiming of addresses**) and server-based assignment.

Note that a solution based on IETF DHCPv6 [REF], for example an extension to it for the assignment of MAC addresses in addition to current functionality, could be used to provide this assignment. This solution for the general case of an IP network on top of an IEEE 802 network will be desirable, but cannot serve as the only solution since it requires IP connectivity, which is not always available in IEEE 802 networks.

Therefore, as summary, the objective of this specification is to define the IEEE 802.1CQ protocol, also known as LAAP (Local Address Assignment Protocol), it must enable the automatic assignment of 48 or 64 MAC addresses in the SAI space as defined in IEEE 802c.

Background

Relation with IEEE 802c

Currently, globally unique MAC addresses are assigned to most IEEE 802 end stations and bridge ports. Increasing use of virtual machines and Internet of Things (IoT) devices could exhaust the global MAC address space if global MAC addresses are assigned. These applications could use the local MAC address space, but in that case some applications

require independent address administration (e.g. virtualization systems and protocol specific address mappings). The IEEE 802c project provides conventions and enable protocols that will allow multiple stations or servers to automatically configure and use local MAC addresses without conflict when multiple administrations share a local address space. Such protocols will allow virtual machines and IoT devices to obtain a local MAC address without centralized local MAC address administration.

IEEE 802c provides an optional local MAC address space structure to allow multiple administrations to coexist. This structure will designate a range of local MAC addresses for protocols using a Company ID (CID) assigned by the IEEE Registration Authority. Another range of local MAC addresses will be designated for assignment by local administrators. IEEE 802c will recommend a range of local MAC addresses for use by IEEE 802 protocols.

Specifically, the IEEE 802c defines the so called SLAP (Structured Local Address Plan) in which 4 ranges or quadrants of local MAC addresses are defined:

- Extended Local (ELI)
- Standard Assigned (SAI)
- Administratively Assigned (AAI)
- Reserved

Each quadrant is defined in base of 4 bits of the MAC address. The least and second least significant bits of the initial octet of a MAC address are designated the M bit and X bit, respectively. The X bit is also referred to as the U/L bit, short for Universal/Local, which identifies how the address is administered (if the bit is 0, the address is universally administered; if it is 1, the address is locally administered). The M bit indicates if the address is unicast (0) or multicast/broadcast (1). The third and fourth least significant bits of the initial octet in the local MAC address are designated the Y bit and Z bit, respectively, as illustrated for a 48-bit address in the next figure.

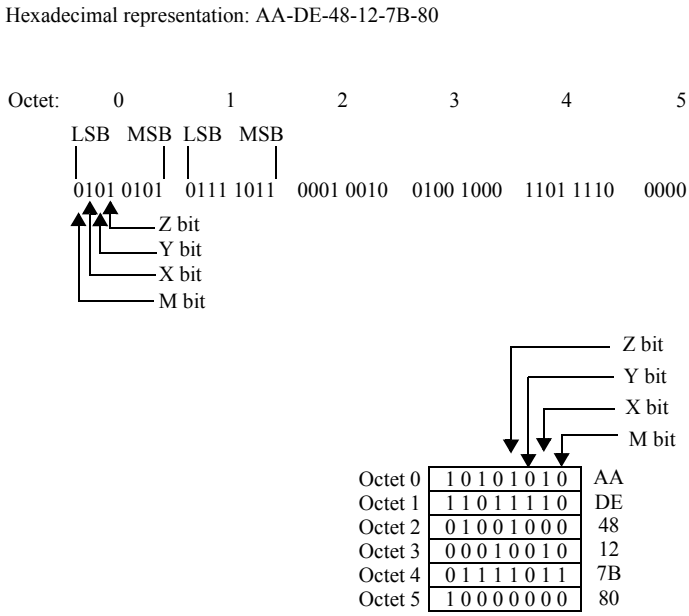

Figure 1: M, X, Y and Z bots lof local MAC address

A local address exists in one of four SLAP quadrants, each identified by a different combination of the Y and Z bits, as indicated in the next table. That table also indicates the SLAP local identifier type specified for each SLAP quadrant. The SLAP local identifier types are specified below.

Table 1: SLAP Quadrants

SLAP Quadrant	Y bit	Z bit	SLAP local identifier type	SLAP local identifier
01	**0**	**1**	Extended Local	ELI
11	**1**	**1**	Standard Assigned	SAI
00	**0**	**0**	Administratively Assigned	AAI
10	**1**	**0**	*reserved*	*reserved*

A SLAP identifier of type “Extended Local” is known as an Extended Local Identifier (ELI). ELIs fall in SLAP Quadrant 01. The X, Y, and Z bits of an ELI are 1,0,1 respectively. An ELI may be used as local MAC address; such an address is known as an ELI address.

The IEEE RA (Registration Authority) uniquely assigns a 24-bit identifier known as the Company ID (CID) 1 to identify a company, organization, entity, protocol, etc., as described in “Guidelines for Use Organizationally Unique Identifier (OUI) and Company ID (CID)”. An ELI is based on an assigned Company ID. Two different lengths of ELI are

specified – ELI-48 is a 48-bit ELI and ELI-64 is a 64-bit ELI

A SLAP identifier of type “Standard Assigned” is known as a Standard Assigned Identifier (SAI). SAIs fall in SLAP Quadrant 11. The X, Y, and Z bits of an SAI are 1,1,1 respectively. An SAI may be used as local MAC address; such an address is known as an SAI address. Specification of the use of the SAI quadrant for SLAP address assignments is reserved for IEEE Std 802.1CQ (this specification).

A SLAP identifier of type “Administratively Assigned” is known as an Administratively Assigned Identifier (AAI). AAIs fall in SLAP Quadrant 00. The X, Y, and Z bits of an SAI are 1,0,0 respectively. An AAI may be used as local MAC address; such an address is known as an AAI address.

Administrators who wish to assign local MAC addresses in an arbitrary fashion (for example, randomly) and yet maintain compatibility with other assignment protocols operating under the SLAP on the same LAN may assign a local MAC address as AAI.

Basic of Multicast and local address assignment

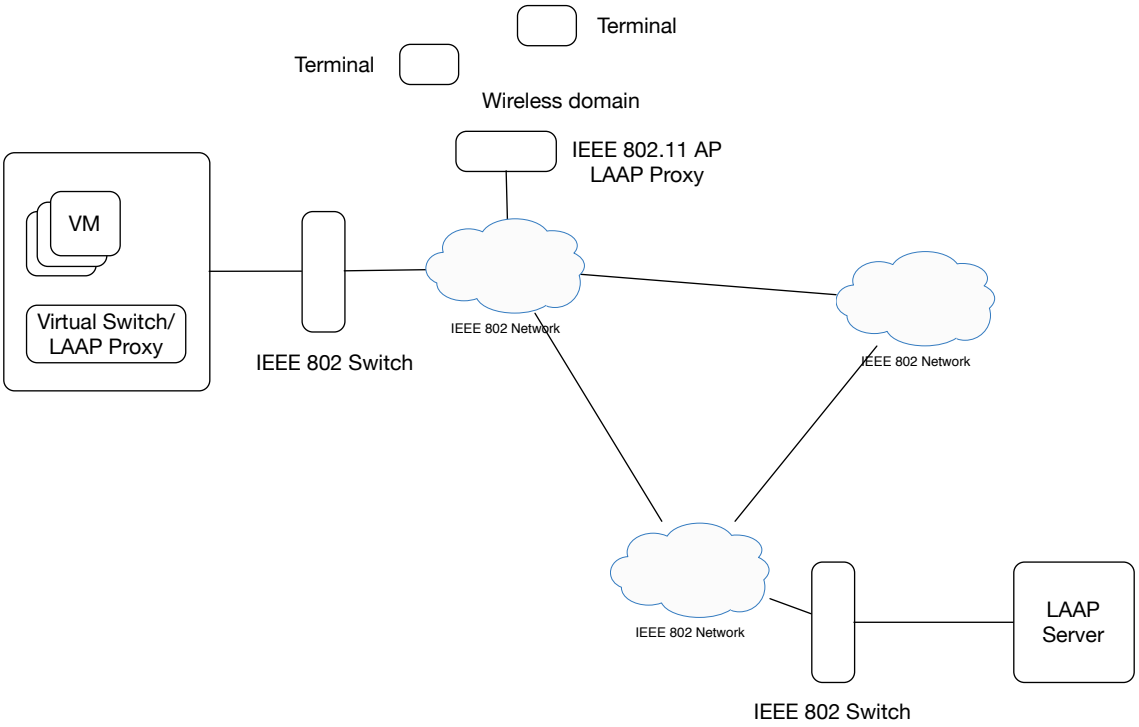

Figure 2: reference scenario

In Figure 2, we present the reference scenario showing a typical deployment of LAAP in an IEEE 802 network. The network is composed by different IEEE 802 links connected by different IEEE 802.1 switches. In Figure 2 there is one LAAP server (note there may be more than one LAAP Server in the network). In addition to the server there are two LAAP

Proxies, the first one is located in the AP connecting wireless terminals to the network. This proxy will provide MAC address assignment to wireless stations attached to it. The MAC addresses assigned to the wireless domain are delegated to the LAAP Proxy by the LAAP server. In addition, there is a second LAAP proxy in the network. This LAAP proxy is located inside the virtual switch running in a virtualization server, e.g., a NFVI in ETSI NFV nomenclature. This LAAP Proxy has been delegated a big chunk of MAC addresses from the LAAP server and provides them to the virtual machines instantiated and connected to it.

A terminal connected to a network such as the one depicted in Figure 2, may use two differentiated mechanisms to obtain a MAC address belonging to the SLAC quadrant as defined in IEEE 802c [REF]. Note that both methods may be deployed simultaneously in the same network:

- Self-Assignment of MAC address: Through this method, which may be supported by specific functionality in the network, an IEEE 802 device connected to the network can self-assign a MAC address, without intervention of the LAAP server. This method is defined in Clause XX.
- Server/Proxy based assignment: Through this method, the terminal is able to get a MAC address delegated from a LAAP Server or Proxy. This method is defined in Clause XX.

Theory of operation

As explained in Clause XX, this document specifies two mechanisms for the LAAC, Self-assignment and Server based assignment. In the following clauses, the theory of operation of each of these mechanisms is explained.
The LAAP Self-Assignment procedure must meet the following requirements:

- Assigning addresses that are locally unique
- Providing for duplicate detection
- Allowing the acquisition of multiple addresses
- Providing fast address assignment
- Responding for low power sleeping device
- Avoiding flooding from device before address assignment
- Allowing an administrator to define specific MAC address assignment policies and addressing plans for the network.

Self-Assignment of MAC addresses

Through this mechanism a station connecting to an IEEE 802-based network is able to obtain a MAC address to be used to communicate in the network. The rationale behind the procedure presented is to enable the network administrator to define the range of addresses to be used for self-assignment. This is required in case the network implements specific L2 addressing plans which may enable novel L2 forwarding mechanisms.

The mechanism is divided in three stages:

- Detection of network capabilities and address space to be used

- Self-assignment of address
- Duplicate address detection through claiming of the self-assigned address

The first phase (Detection of network capabilities and address space to be used) consists on the discovery of the capabilities regarding local MAC addresses of the network. The station, after attaching to the network, requires of information regarding the support of LAAP in the network, if the network supports self-assignment or server based. This is achieved by listening to specific messages sent by the infrastructure (e.g., broadcasted by the first LAAP compatible switch the station is attached to). Messages and procedures for detecting the capabilities of the network are defined in Clause XX.

In case LAAP Self-Assignment is supported, the station needs to discover if there is some specific range of addresses defined to perform Self-assignment. The detection is performed through listening to specific messages, defined in Clause XX, which indicate the value for certain bits of the 48 or 64 bit address space. For the rest of the document we will refer to the specific set of fixed value bits defined by the administrator as prefix.
Once the Station has identified the value for the prefix, the station is able to randomly select a value for the rest of bits and assign the resulting address to the interface.
At this point of time, the self-assigned address cannot be assumed to be unique in the 802 domain. For this reason a Duplicate Address Detection (DAD) mechanism must be employ to assure its uniqueness.

LAAC Duplicate Address Detection mechanism

The DAD mechanism specified in this document is very similar to the DAD mechanism for IPv6 specified in Pv6 Stateless Address Auto-Configuration (SLAAC) [REF]. It is based on a set of messages which are used to probe the address just self-assigned by the station.
The procedure for Claiming the address is specified in the following figure:

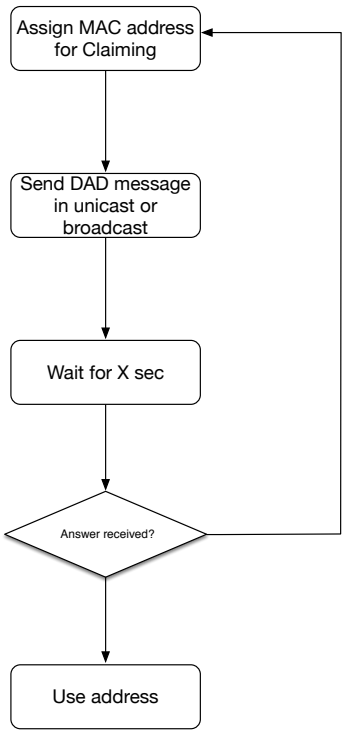

Figure 3: DAD procedure

The messages related to this procedure are specified in Clause XX. The procedure for DAD is the following:

- The station sends a DAD request as specified in Clause XX. The source address of the DAD request must be set to the self-assigned address. This message can be sent using three possible choices for source address:
    - Use of broadcast address (ff:ff:ff:ff:ff:ff). This solution will cause the network to flood unnecessary messages, since all stations in the LAN will receive the message. In this case the source MAC address will be set to the claimed unicast address or to the broadcast address (as recommended by IEEE RA for NULL addresses).
    - Unicast to the MAC address claimed. A message is sent in unicast to the address to be claimed. In this case the stations receiving the message (with a duplicate address) will answer and the duplication will be detected. The drawback is that the IEEE 802.1CQ server will not receive it. In this case the source address of the DAD message must be a one-usage random address in the SAI/AAI space or the broadcast address (as recommended by IEEE RA for NULL addresses).
    - Use of a multicast group, such as the one used for the solicited multicast in IPv6. When a station self-assigns a MAC address, then it joins a multicast group such as the 33:33:xx:xx:xx:xx, where the last 4 bytes correspond to the last 4 bytes of the self-assigned MAC address. In this way, if there is no station subscribed to the group, the switches will not forward the packet and the flooding is reduced. In case a DAD message addressed to a multicast address is received by a station, it must check if the target address within the

message is the one configured in the interface. This is needed since multiple stations with different MAC addresses (sharing the last 4 bytes) can be subscribed to the same group.

- Wait for a pre-defined period of time.
- If a station receives a DAD request with source address assigned to its interface, it must answer with a DAD response (as defined in Clause XX) in unicast to the source address of the received DAD request.
- In case a DAD response is received, this means the self-assigned address is not unique in the network. The originating station must reselect a new MAC address and perform the DAD procedure for it.

In any case, if a Claiming address space TLV (see Clause XX) is received, specifying a different Claiming address space than the one used, the claiming process must be aborted and a new MAC address following the rules indicated in the received Claiming address space TLV must be formed and used for the DAD procedure.

In addition, a faster procedure, known as Optimistic Duplicate Address Detection may be used. In this procedure, the MAC address can be used immediately after sending the message but in the case a DAD response is received, the station must stop using the address and perform a Claiming procedure again.

Please note that the impact on the network of using a duplicated address may be high depending on the complexity of the network. In the case of big networks, having duplicate MAC addresses may cause a disruption of the Spanning Tree or Shortest Path Bridging algorithms, potentially disrupting the network seriously.

Message formats

This Clause is devoted to present the different messages used for the procedures defined in IEEE 802.1CQ.
There are several options to encapsulate the protocol:

- encapsulated as a new protocol over IEEE 802.2 LLC
- encapsulated as a new TLV over LLDP

If the protocol is specified on top of IEEE 802.2 LLC, it can be encapsulated directly over the LLC header or using a SNAP header (which makes it compatible with Ethernet).

Messages related to the Self-configuration of MAC addresses

Claiming address space TLV

This TLV provides information on the prefix to be used at MAC layer to self-assign addresses through claiming.

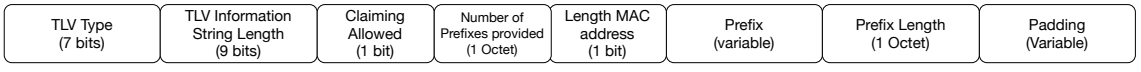

Figure 4: Claiming address space TLV

A station receiving this TLV will be able to self-assign an address belonging to a prefix provided by the administrator of the LAN. First, the Claiming Allowed bit indicates if Claiming is allowed, if this bit is set to 0 Claiming is not allowed and the rest of the message will be empty. In this case the message will contain an all zero octet for Number of Prefixes Provided and padding as needed.

The number of prefixes provided indicates the number of prefixes which are advertised in the messages. After this field, the message repeats the three next fields the number of times indicated in the Number of Prefixes Provided field. Length of MAC address corresponds to 48 if 0 or 64 bits if 1. Finally, Prefix corresponds to a 48 or 64 bit MAC address and the prefix length indicates the network part of the prefix.

This allows the system administrator to deploy meaningful MAC addressing schemes that follow a certain hierarchy or structure, even if the address is self-assigned.

DAD Messages

DAD Request/Response

Figure XX, presents the format of the DAD request/response message

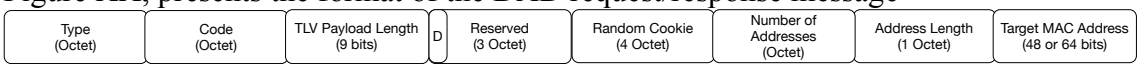

Figure 5: DAD request

The type and code value must be agreed within the standard. The TLV Payload Length contains the information on the overall size of the payload. It is considered 9 bits in order to be compatible with the maximum size of LLDPs messages, so this format is compatible with LLDP (changing the Type and Code fields to a TLV type field of 7 bits) and LLC/SNAP encapsulation. The Reserved field, of 3 octets serves as a bitmap buffer for future protocol extensions. The most significant bit is denoted as the D (for duplicate) bit. This bit is set to 0 in case the message is a request and set to 1 if a station is answering the message, i.e., there is a duplicate MAC conflict.
The Random Cookie is used to differentiate messages, if there are multiple stations with same MAC address, there will be multiple DAD messages in the network and this serves as a mechanism to differentiate them. This is a possible solution for the corner case where multiple stations select the same claiming addresses simultaneously.
The Number of addresses field indicates how many addresses are claimed in this message. Finally, the Address length and Target MAC address contain the length and MAC address subject of the DAD procedure.

The above definition of the payload can be encapsulated by the two mechanisms defined above, using LLC or LLDP.

Hence, the DAD procedure is based on the sending of the DAD request, with the D bit set to 0 and wait for some time (to be defined) until a DAD request, with D bit set to 1, is received or the timer expires.

In case multiple addresses are claimed, the station may choose between using 1 message per address sent in unicast or a bulk message sent to broadcast. Unicast answers are expected for each duplicated MAC address detected.

Messages related to Server-based assignment

Server/Proxy Address TLV

This TLV provides information on the address of the server or proxy to be used for MAC address assignment. The TLV simply indicates what is the address to be used to reach the IEEE 802.1CQ server/proxy.

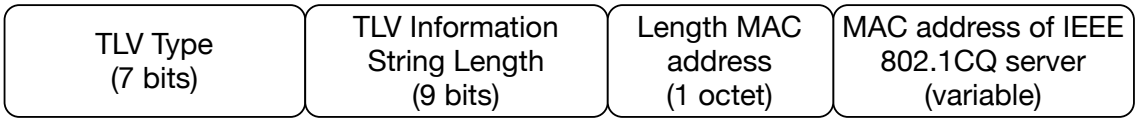

Figure 6: IEEE 802.1CQ Server/Proxy Address